UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/717,521	11/21/2000	Herman Rodriguez	A US9-2000-0560-US1	1827

7590 01/02/2004

IBM Corporation
Intellectual Property Law Dept.
11400 Burnet Road 4054
Austin, TX 75758

EXAMINER	
BROWN, VERNAL U	

ART UNIT	PAPER NUMBER
2635	6

DATE MAILED: 01/02/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/717,521	RODRIGUEZ ET AL.	
	Examiner	Art Unit	
	Vernal U Brown	2635	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-78* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-78* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

This action is responsive to amendment filed October 22, 2003.

Response to Amendment

The examiner has acknowledged the amended claims 1, and 29.

Response to Arguments

Applicant's arguments with respect to claims 1-78 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 29, 33, 36, 37, 41-43, and 46-50 are rejected under 35 U.S.C. 102(e) as being anticipated by Waggamon et al. U.S Patent 6049289.

Regarding claim 29, Waggamon et al. teaches an apparatus for operating an electronic locking device using a wireless communication device (figure 1), comprising: means for receiving a master key code (secret key) from a master key supplier (figure 1); means for generating a secondary key code, from the master key code (col. 4 lines 61-65); and means for

transmitting the secondary code to the wireless communication device (42), wherein the secondary key code is to operate the electronic locking device (col. 8 lines 18-21).

Regarding claim 33 and 37, Waggamon et al. teaches means for transmitting the secondary code by a wireless communication link (figure 1).

Regarding claim 36, Waggamon et al. teaches the wireless communication device is a wireless transmitter (40).

Regarding claim 41, Waggamon et al. teaches the electronic locking device is preprogrammed to accept the key code (col. 6 lines 41-44).

Regarding claim 42, Waggamon et al. the wireless communication device transmit the secondary code to the receiver of the locking device (figure 2) and the key code is decoded and transmitted to the drive mechanism (64) of the lock of the garage door (col. 7 lines 55-56). The code to the lock is therefore transmitted at a different (remote) time than the secondary code to the wireless device.

Regarding claim 43, Waggamon et al. teaches means (54) for receiving a key code from the wireless communication device (figure 2), means for authenticating the key code (col. 8 lines 16-19), and means for transmitting a command to open the electronic locking device (col. 8 lines 19-21).

Regarding claim 46, Waggamon et al. teaches authenticating the key code by performing a comparison of the key code to information stored in the key code table (col. 8 lines 16-18).

Regarding claim 47, Waggamon et al. teaches the entry for the locking device includes device identification information (col. 4 lines 58-59).

Regarding claim 48, Waggamon et al. teaches a wireless communication device (40) which is conventionally owned by the user.

Regarding claim 49, Waggamon et al. teaches encoding (encryption) of the secondary code (col. 5 lines 10-12).

Regarding claim 50, Waggamon et al. teaches means for recording secondary codes used to the locking device (col. 18 lines 16-18).

Claims 56-57, 59, 60-62, 64-66, 68-71, and 73-78 are rejected under 35 U.S.C. 102(e) as being anticipated by Kuchharczyk et al. U.S Patent 6300873.

Regarding claims 56, 75 and 78, Kucharczyk et al. teaches a method of operating an electronic locking device using a wireless communication device (col. 4 lines 47-49), comprising:

receiving a master key and generating a secondary key code (master code) (col. 7 lines 54-56)

requesting a secondary key code from a key code supplier (col. 7 lines 11-13);

receiving the secondary key code associated with the electronic locking device (col. 5 lines 14-15), the secondary key code having been generated based on a master key code unique seed (master code) (col. 7 lines 54-56); and

transmitting the secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key code (col. 4 lines 38-50). Kucharczyk et al. teaches the key code is supplied by a server and the operation of the locking mechanism is control by the server (col. 7 lines 23-37) which inherently includes a computer product.

Regarding claims 57, 66, and 76 Kuchharczyk et al. teaches a method of operating an electronic locking device using a wireless communication device (col. 4 lines 47-49), comprising:

requesting a secondary key code from a key code supplier (col. 7 lines 11-13);

receiving the secondary key code associated with the electronic locking device (col. 5 lines 14-15), the secondary key code having been generated based on a master key code unique seed (master code) (col. 7 lines 54-56); and

transmitting the secondary key code to the electronic locking device, wherein the electronic locking device is operated in response to receiving the secondary key code (col. 4 lines 38-50).

Regarding claims 59 and 68, Kuchharczyk et al. teaches the wireless communication device is a wireless transmitter (90).

Regarding claims 60-61 and 70, Kucharczyk et al. teaches attaching key code to an electronic mail (col. 9 lines 55-59). The sending of the code at a remote time from the use of the secondary code is implied because the code must be received before it can be used.

Regarding claims 62 and 71, Kucharczyk et al. teaches the server provides access codes to the storage device (col. 6 lines 27-30) which means that the locking device must be preprogrammed to accept the key codes.

Regarding claims 64-65 and 73-74, Kucharczyk et al. teaches the key supplier (server) detecting codes that are never used and automatically canceling (deleting) such codes (col. 8 lines 49-53).

Regarding claim 69, Kucharczyk et al. teaches attaching key code to an electronic mail (col. 9 lines 55-59)

Regarding claim 77, Kucharczyk et al. teaches receiving a key code from the wireless communication device and transmitting a command to operate the locking device if the key code is authentic (col. 4 lines 51-65).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 1, 5, 8-11, 13-15, 18, 20, 22-25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6570488 in view of Bruwer U.S Patent 6166650.

Regarding claim 1, Kucharczyk et al. teaches a method of operating an electronic locking device using a wireless communication device (col. 10 lines 49-66). Kucharczyk et al. also teaches providing an access code generated from a unique seed (master code) (col. 7 lines 54-56). Kucharczyk et al. is however silent on teaching receiving a master key code from a master key supplier and generating a secondary key code from the master key code and transmitting the secondary key code to the wireless communication device. Bruwer in an art related invention in the same field of endeavor of security system teaches receiving a master key

code from a master key supplier and generating a secondary key code from the master key code (col. 7 lines 54-57) and transmitting the secondary key code to the (decoder) wireless communication device (col. 8 lines 56-64).

It would have been obvious to on of ordinary skill in the art to receive a master key code from a master key supplier and generating a secondary key code from the master key code and transmitting the secondary key code to the wireless communication device in Kucharczyk et al. as evidenced by Bruwer because Kucharczyk et al. suggests a method of operating an electronic locking device using a wireless communication device and providing an access code generated from a unique seed (master code) and Bruwer teaches teaches receiving a master key code from a master key supplier and generating a secondary key code from the master key code and transmitting the secondary key code to the (decoder) wireless communication device.

Regarding claims 5 and 9, Kucharczyk et al. teaches the electronic locking device using a wireless or wired communication link (col. 12 lines 50-51).

Regarding claim 8, Kucharczyk et al. teaches the wireless communication device (90) is a wireless transmitter (figure 7).

Regarding claims 10-11 and 14, Kucharczyk et al. teaches attaching key code to an electronic mail (col. 9 lines 55-59). The sending of the code at a remote time from the use of the secondary code is implied because the code must be received before it can be used.

Regarding claim 13, Kucharczyk et al. teaches the server provides access codes to the storage device (col. 6 lines 27-30) which means that the locking device must be preprogrammed to accept the key codes.

Regarding claim 15, Kucharczyk et al. in view of Bruwer teaches receiving a key code from the wireless communication device and transmitting a command to operate the locking device if the key code is authentic (col. 4 lines 51-65).

Regarding claim 18, Kucharczyk et al. teaches authenticating the key code by performing a comparison of the key code to information stored in the key code table (col. 10 lines 5-8).

Regarding claim 20, Kucharczyk et al. teaches the wireless communication device is own by the user (col. 4 lines 51-52).

Regarding claim 22, Kucharczyk et al. teaches maintaining a record of secondary key codes used to access the locking device (figure 4).

Regarding claim 23, Kucharczyk et al. teaches using a random number to generate a key code (col. 7 lines 54-55).

Regarding claim 24, Kucharczyk et al. teaches the authentication of the key coded depends on activation/expiration time of the key code (col. 8 lines 49-57).

Regarding claim 25, Kucharczyk et al. teaches the use of the internet to supply key code (figure 5).

Claims 2, 19, 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6570488 in view of Bruwer U.S Patent 6166650 and further in view of Hyatt, Jr. et al. U.S Patent 5745044.

Regarding claims 2, 19, 21 Kucharczyk et al. in view of Bruwer teaches a device identification portion associated to the secondary code (col. 10 lines 45-48) but is silent on teaching the secondary key includes an activation/expiration portion, a time of issue portion and

a time of last use portion. Hyatt, Jr. et al. in an art related Electronic Security System teaches a key which stores information including an activation/expiration portion, a time of issue portion and a time of last use portion (col. 4 lines 52-59).

It would have been obvious to one of ordinary skill in the art to for the secondary key to includes an activation/expiration portion, a time of issue portion and a time of last use portion in Kucharczyk et al. in view of Bruwer as evidenced by Hyatt, Jr. et al. because Kucharczyk et al. in view of Bruwer suggests a device identification portion associated to the secondary code and Hyatt, Jr. teaches including an activation/expiration portion, a time of issue portion and a time of last use portion in the key code in order to improver the security of the access system.

Claims 3- 4 and 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6570488 in view of Bruwer U.S Patent 6166650 and further in view of Brinkmeyer et al. U.S Patent 5838251.

Regarding claim 3, Kucharczyk et al. in view of Bruwer teaches the wireless device receiving the master key code (unique seed) (col. 7 lines 54-56) and transmitting key code over a network (figure 5) but is not explicit in teaching receiving the master key code over a network. Brinkmeyer et al. in an art related invention for programming a key code teaches receiving a master key code (encoded data) from a master key supplier (20) and the master code is received by a network as shown in figure 3 and (col. 9 lines 42-45).

It would have been obvious to one of ordinary skill in the art to receive the master key code over a network in Kucharczyk et al. in view of Bruwer as evidenced by Brinkmeyer et al. because Kucharczyk et al. in view of Bruwer suggests the wireless device receiving the master

key code (unique seed) and transmitting key code over a network and Brinkmeyer et al. teaches transmitting a master key code to a wireless device over a network.

Regarding claim 4, Kucharczyk et al. in view of Bruwer teaches the wireless device receiving the master key code (unique seed) (col. 7 lines 54-56) but is silent on teaching sending a master key code request to the master key supplier identifying one or more of a key supplier identifier, a product code of the electronic locking device. Brinkmeyer et al. in an art related invention for programming a key code teaches sending a master key code (encoded data) request to the master key supplier and the master key request identifying a product code of the electronic locking device (col. 6 lines 2-5).

It would have been obvious to one ordinary skill in the art to send a master key code request to the master key supplier identifying one or more of a key supplier identifier, a product code of the electronic locking device in Kucharczyk et al. in view of Bruwer as evidenced by Brinkmeyer et al. because Kucharczyk et al. in view of Bruwer suggests the wireless device receiving the master key code and Brinkmeyer et al. teaches sending a master key code (encoded data) request to the master key supplier and the master key request identifying a product code of the electronic locking device.

Regarding claims 26-27, Kucharczyk et al. in view of Bruwer teaches providing update to the server regarding the locking device (col. 8 lines 6-9) but is silent on teaching polling the locking device and receiving status information from the electronic locking device. Brinkmeyer et al. in an art related invention for programming a key code teaches polling the electronic

locking device and receiving status information from the electronic locking device (col. 10 lines 47-47) and the status information includes the current status of the lock (col. 10 lines 47-54).

It would have been obvious to one of ordinary skill in the art to poll the locking device and receiving status information from the electronic locking device in Kucharczyk et al. in view of Bruwer as evidenced by Brinkmeyer et al. because Kucharczyk et al. in view of Bruwer suggests providing update to the server regarding the locking device and Brinkmeyer et al. teaches providing update information by polling the electronic locking device and receiving status information from the electronic locking device.

Regarding claim 28, Kucharczyk et al. teaches operating the locking device based on the status information based on when the codes are used (col. 8 lines 49-55).

Claims 6-7 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6570488 in view of Bruwer U.S Patent 6166650 and further in view of Gonzales et al. U.S Patent 5936544.

Regarding claims 6-7, Kucharczyk et al. in view of Bruwer teaches transmitting the secondary key code to the locking device (col. 2 lines 54-61) but is silent on teaching transmitting the secondary code to the locking device includes transmitting the secondary key code based on a network address. Gonzales et al. in an art related wireless access system teaches the transmission of an access code based on the network address of the locking device (col. 5 lines 2-8).

It would have been obvious to one of ordinary skill in the art to transmit the secondary code to the locking device including transmitting the secondary key code based on a network address in Kucharczyk et al. in view of Bruwer as evidenced by Gonzales et al. because Kucharczyk et al. in view of Bruwer suggests transmitting identifying means of the locking mechanism and Gonzales et al. teaches transmitting identifying means of lock mechanism which include transmitting the network address of the locking mechanism.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6570488 in view of Bruwer U.S Patent 6166650 and further in view of Henderson et al. U.S Patent 4947163.

Regarding claim 12, Kucharczyk et al. in view of Bruwer teaches the reprogramming (updating) of a lock device (col. 13 line 55) but is silent on teaching confirming reprogramming of the electronic locking device with a confirmation message. Henderson et al. in an art related invention in the same field of endeavor of electronic security teaches transmitting of a confirmation messages after the successful completion of data transfer between the key and the electronic locking device (col. 10 lines 39-45).

It would have been obvious to one of ordinary skill in the art to confirm reprogramming of the electronic locking device with a confirmation message in Kucharczyk et al. in view of Bruwer as evidenced by Henderson et al. because Kucharczyk et al. in view of Bruwer suggests the reprogramming of a locking device and Henderson et al. teaches transmitting of a confirmation messages after the successful completion of data transfer between the key and the electronic locking device.

Claims 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6300873 in view of Bruwer U.S Patent 6166650 and further in view of Henry et al. U.S Patent 5774059.

Regarding claims 16-17, Kucharczyk et al. in view of Bruwer teaches receiving a key code from the wireless communication device and transmitting a command to operate the locking device if the key code is authentic (col. 4 lines 51-65) but is silent on teaching determining if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode. One skilled in the art recognizes that it is convention practice to determine if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode as evidenced by Henry et al. (col. 12 lines 18-24).

It would have been obvious to one of ordinary skill in the art to determining if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode in Kucharczyk et al. in view of Bruwer as evidenced by Henry et al. because Kucharczyk et al. in view of Bruwer teaches a locking device which requires a correctly coded key and one skilled in the art recognizes that it is convention practice to determine if a number of attempts to operate the electronic locking device exceeds a threshold within a

predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode as evidenced by Henry et al.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Waggamon et al. U. S Patent 6049289 in view of Hyatt, Jr. et al. U.S Patent 5745044.

Regarding claim 30, Waggamon et al. et al. teaches a device identification portion associated to the secondary code (col. 4 lines 58-59) but is silent on teaching the secondary key includes an activation/expiration portion, a time of issue portion and a time of last use portion. Hyatt, Jr. et al. in an art related Electronic Security System teaches a key which stores information including an activation/expiration portion, a time of issue portion and a time of last use portion (col. 4 lines 52-59).

It would have been obvious to one of ordinary skill in the art to for the secondary key to includes an activation/expiration portion, a time of issue portion and a time of last use portion in Waggamon et al. et al. as evidenced by Hyatt, Jr. et al. because Waggamon et al. et al. suggests a device identification portion associated to the secondary code and Hyatt, Jr. teaches including an activation/expiration portion, a time of issue portion and a time of last use portion in the key code in order to improver the security of the access system.

Claim 31-32 and 54-55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waggamon et al. U. S Patent 6049289 in view of Brinkmeyer et al. U.S Patent 5838251.

Regarding claim 31, Waggamon et al. et al. teaches receiving the master key code from a master key supplier (figure 3) but is silent on teaching receiving the master key by a network.

Brinkmeyer et al. in an art related invention for programming a key code teaches receiving a master key code (encoded data) from a master key supplier (20) and the master code is received by a network as shown in figure 3 and (col. 9 lines 42-45).

It would have been obvious to one of ordinary skill in the art to receive the master key by a network in Waggamon et al. et al. as evidenced by Brinkmeyer et al. because Waggamon et al. et al. suggests receiving the master key code from a master key supplier and Brinkmeyer et al. teaches using a network to supply the master key.

Regarding claim 32, Waggamon et al. et al. teaches the wireless device receiving the master key code (col. 4 lines 61-65) but is silent on teaching sending a master key code request to the master key supplier identifying one or more of a key supplier identifier, a product code of the electronic locking device. Brinkmeyer et al. in an art related invention for programming a key code teaches sending a master key code (encoded data) request to the master key supplier and the master key request identifying a product code of the electronic locking device (col. 6 lines 2-5).

It would have been obvious to one ordinary skill in the art to send a master key code request to the master key supplier identifying one or more of a key supplier identifier, a product code of the electronic locking device in Waggamon et al. et al. as evidenced by Brinkmeyer et al. because Waggamon et al. et al. suggests the wireless device receiving the master key code and Brinkmeyer et al. teaches sending a master key code (encoded data) request to the master key supplier and the master key request identifying a product code of the electronic locking device.

Regarding claims 54-55, Waggamon et al. is silent on teaching polling the locking device and receiving status information from the electronic locking device. Brinkmeyer et al. in an art related invention for programming a key code teaches polling the electronic locking device and receiving status information from the electronic locking device (col. 10 lines 47-47) and the status information includes the current status of the lock (col. 10 lines 47-54).

It would have been obvious to one of ordinary skill in the art to poll the locking device and receiving status information from the electronic locking device in Waggamon et al. et al. as evidenced by Brinkmeyer et al. because Waggamon et al. suggests updating the code by learning new codes and Brinkmeyer et al. teaches providing update information by polling the electronic locking device and receiving status information from the electronic locking device.

Claims 34-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waggamon et al. U. S Patent 6049289 in view of Gonzales et al. U.S Patent 5936544.

Regarding claims 34-35, Waggamon et al. is silent on teaching transmitting the secondary code to the locking device includes transmitting the secondary key code based on a network address. Gonzales et al. in an art related wireless access system teaches the transmission of an access code based on the network address of the locking device (col. 5 lines 2-8).

It would have been obvious to one of ordinary skill in the art to transmit the secondary code to the locking device including transmitting the secondary key code based on a network address in Waggamon et al. as evidenced by Gonzales et al. because Waggamon et al. et al. suggests transmitting identifying means of the locking mechanism and Gonzales et al. teaches

transmitting identifying means of lock mechanism which include transmitting the network address of the locking mechanism.

Claims 38-39 and 51-53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waggamon et al. U. S Patent 6049289 in view of Kucharczyk et al. U.S Patent 6300873.

Regarding claims 38-39, Waggamon et al. teaches transmitting the key code to the wireless device (figure 3) but is silent on teaching attaching key code to an electronic mail. Kucharczyk et al. in an art related invention in the same field of endeavor or electronic lock teaches attaching key code to an electronic mail (col. 9 lines 55-59). The sending of the code at a remote time from the use of the secondary code is implied because the code must be received before it can be used.

It would have been obvious to one of ordinary skill in the art to attach the key code to an electronic mail in Waggamon et al. as evidenced by Kucharczyk et al. because Waggamon et al. suggests transmitting the key code to the wireless device and Kucharczyk et al. teaches attaching key code to an electronic mail.

Regarding claim 51, Waggamon et al. teaches means of generating a secondary code from a master key code (col. 4 lines 61-65) but is silent on teaching using a random number generator. Kucharczyk et al. in an art related invention in the same field of endeavor or electronic lock teaches using a random number to generate a key code (col. 7 lines 54-55).

It would have been obvious to one of ordinary skill in the art to use a random number generator to generate the secondary code in Waggamon et al. as evidenced by Kucharczyk et al

because Waggamon et al suggests means of generating a secondary code from a master key code and Kucharczyk et al. teaches using a random number to generate a key code.

Regarding claims 52-53, Waggamon et al. teaches authenticating the key code (col. 8 lines 16-18) but is silent on teaching but is silent on teaching determining an activation/expiration time of the key code and determining if a current time is within an activation/expiration time. Kucharczyk et al. in an art related invention in the same field of endeavor or electronic lock teaches the authentication of the key coded depends on activation/expiration time of the key code (col. 8 lines 49-57).

It would have been obvious to one of ordinary skill in the art to determine an activation/expiration time of the key code and determining if a current time is within an activation/expiration time in Waggamon et al. as evidenced by Kucharczyk et al. because Waggamon et al. suggests teaches authenticating the key code and Kucharczyk et al. teaches authenticating the key code for a limited time period by monitoring the activation/expiration time of the key code.

Claim 40 is rejected under 35 U.S.C. 103(a) as being unpatentable over Waggamon et al. U. S Patent 6049289 in view of Henderson et al. U.S Patent 4947163.

Regarding claim 40, Waggamon et al. teaches the reprogramming of a lock device (col. 6 lines 14-17) but is silent on teaching confirming reprogramming of the electronic locking device with a confirmation message. Henderson et al. in an art related invention in the same field of endeavor of electronic security teaches transmitting of a confirmation messages after the

successful completion of data transfer between the key and the electronic locking device (col. 10 lines 39-45).

It would have been obvious to one of ordinary skill in the art to confirm reprogramming of the electronic locking device with a confirmation message in Waggamon et al. as evidenced by Henderson et al. because Waggamon et al. in view of Bruwer suggests the reprogramming of a locking device and Henderson et al. teaches transmitting of a confirmation messages after the successful completion of data transfer between the key and the electronic locking device.

Claims 44-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Waggamon et al. U. S Patent 6049289 U.S Patent 6570488 in view of Henry et al. U.S Patent 5774059.

Regarding claims 44-45, Waggamon et al. teaches receiving a key code from the wireless communication device and transmitting a command to operate the locking device (col. 8 lines 16-21) but is silent on teaching determining if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode. One skilled in the art recognizes that it is convention practice to determine if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode as evidenced by Henry et al. (col. 12 lines 18-24).

It would have been obvious to one of ordinary skill in the art to determining if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down

mode and a freeze mode in Waggamon et al. as evidenced by Henry et al. because Waggamon et al. suggests a locking device which requires a correctly coded key and one skilled in the art recognizes that it is convention practice to determine if a number of attempts to operate the electronic locking device exceeds a threshold within a predetermined period of time and placing the electronic lock in a safety mode which is one of a slow down mode and a freeze mode as evidenced by Henry et al.

Claim 58 is rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6300873 in view of Bruwer U.S Patent 6166650 and further in view of Hyatt, Jr. et al. U.S Patent 5745044.

Regarding claim 58 is Kucharczyk et al. teaches a device identification portion associated to the secondary code (col. 10 lines 45-48) but is silent on teaching the secondary key includes an activation/expiration portion, a time of issue portion and a time of last use portion. Hyatt, Jr. et al. in an art related Electronic Security System teaches a key which stores information including an activation/expiration portion, a time of issue portion and a time of last use portion (col. 4 lines 52-59).

It would have been obvious to one of ordinary skill in the art to for the secondary key to includes an activation/expiration portion, a time of issue portion and a time of last use portion in Kucharczyk et al. as evidenced by Hyatt, Jr. et al. because Kucharczyk et al. in view of suggests a device identification portion associated to the secondary code and Hyatt, Jr. teaches including an activation/expiration portion, a time of issue portion and a time of last use portion in the key code in order to improver the security of the access system.

Claims 63, 67, and 72 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kucharczyk et al. U.S Patent 6300873 in view of Bruwer U.S Patent 6166650 and further in view of Hyatt, Jr. et al. U.S Patent 5745044.

Regarding claims 63, 67, and 72, Kucharczyk et al. teaches a device identification portion associated to the secondary code (col. 10 lines 45-48) but is silent on teaching the secondary key includes an activation/expiration portion, a time of issue portion and a time of last use portion. Hyatt, Jr. et al. in an art related Electronic Security System teaches a key which stores information including an activation/expiration portion, a time of issue portion and a time of last use portion (col. 4 lines 52-59).

It would have been obvious to one of ordinary skill in the art to for the secondary key to includes an activation/expiration portion, a time of issue portion and a time of last use portion in Kucharczyk et al. as evidenced by Hyatt, Jr. et al. because Kucharczyk et al. suggests a device identification portion associated to the secondary code and Hyatt, Jr. teaches including an activation/expiration portion, a time of issue portion and a time of last use portion in the key code in order to improver the security of the access system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Vernal U Brown whose telephone number is 703-305-3864. The examiner can normally be reached on M-Th, 8:30 AM-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael Horabik can be reached on 703-305-4704. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9314.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-4750.

Vernal Brown
December 23, 2003

BRIAN ZIMMERMAN
PRIMARY EXAMINER